

# Cyber-Physical Modeling and Analysis for a Smart and Resilient Grid

(Open FOA 670-5143)

Peter W. Sauer

January 14, 2015



ILLINOIS  
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Oregon State  
UNIVERSITY



PowerWorld  
Corporation



RUTGERS  
UNIVERSITY

# Project Objectives (1)

- ▶ **Vision:** Improve operational resiliency in the face of cyber threats
- ▶ **Objectives:**
  - Fuse information from cyber network and physical power network to ***improve security and reliability of the grid***
  - Produce concrete analysis that quantifies how cyber risks can have a real and significant impact
  - Help organizations better evaluate threats and develop countermeasures
- ▶ **Approach:** Combined modeling and analysis of the cyber-physical system rather than dealing with them separately
  - Managing their resiliency separately worked reasonably well for random or accidental faults and failures

# Project Objectives (2)

---

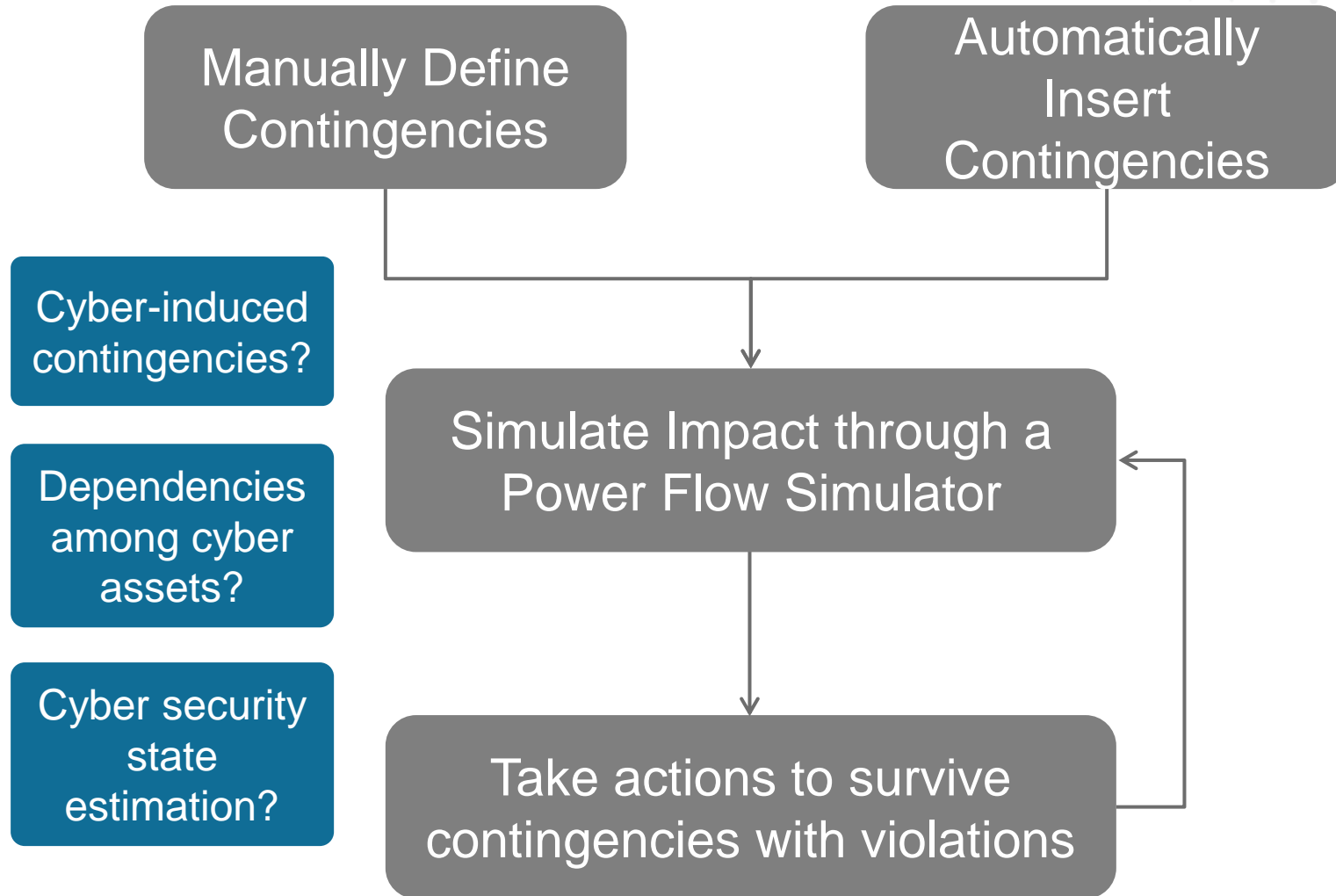
## ► Challenges:

- Identifying cyber-physical dependencies that need to be captured
- Modeling cyber-physical threats and level of detail needed
- Coming up with a modeling and analysis framework
  - efficient, useful

## ► Outcomes:

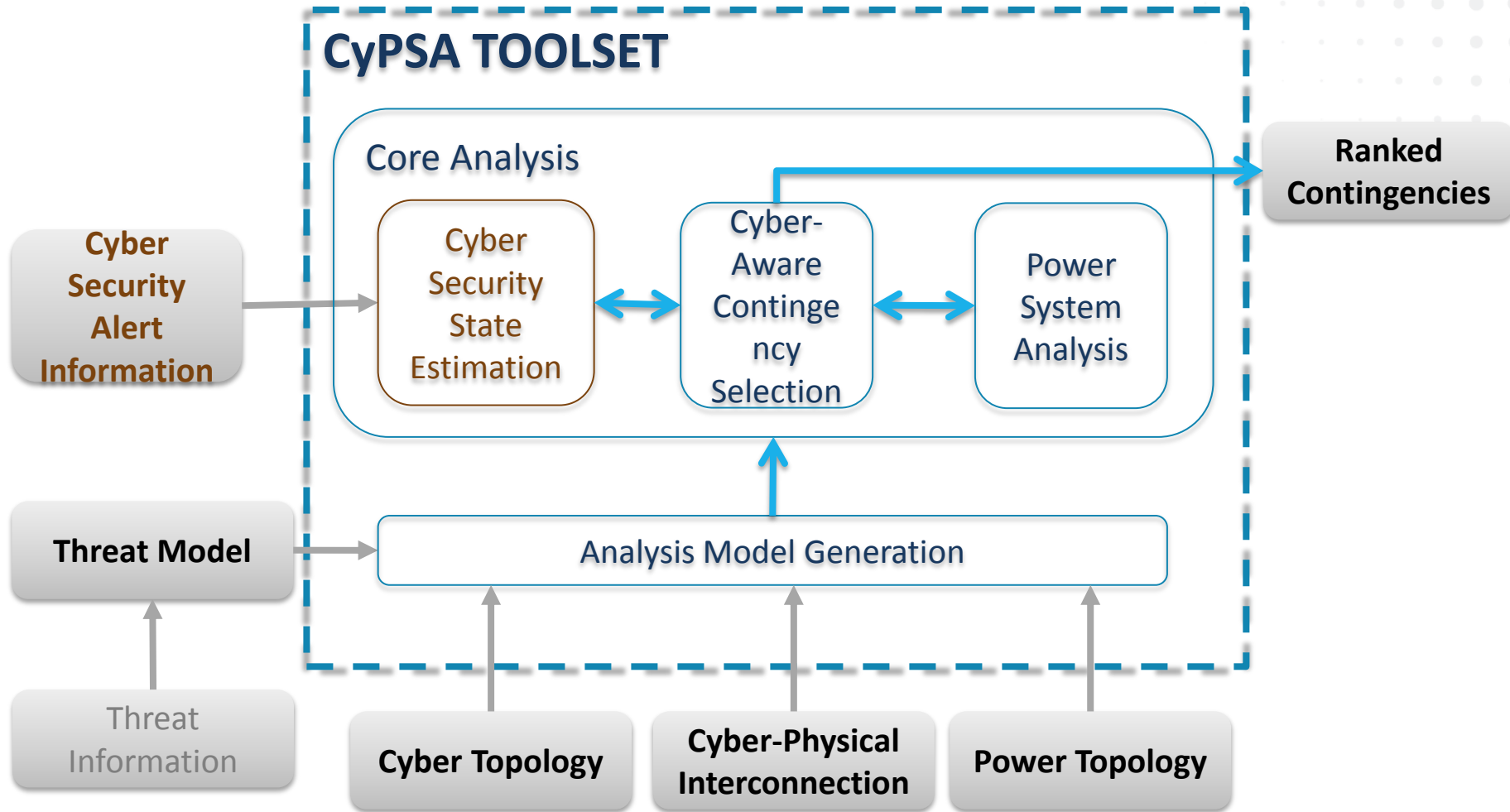
- Cyber-physical models and analysis tools
  - model of connections and dependencies of **cyber** and **physical** systems
  - account for impact of cyber threats on grid reliability
  - **What-if scenario analysis** and **prioritization** of system-hardening and security patching efforts
  - Target Application: Contingency Analysis

# Concept Overview (1)



# Concept Overview (2)

## ► Cyber-Physical Security Analysis (CyPSA)



# Team

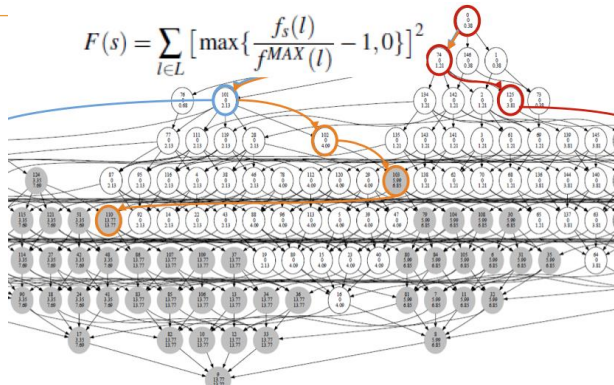
- University of Illinois
  - Robin Berthier
  - Kate Davis
  - David Nicol
  - Edmond Rogers
  - Bill Sanders
  - Pete Sauer
- Oregon State University
  - Rakesh Bobba
- PowerWorld Corp.
  - Matt Davis
- Rutgers University
  - Saman Zonouz
- Interdisciplinary Team
  - Power System Modeling & Analysis (Pete, Kate, Matt)
  - System Security (Rakesh, Robin, Saman, David, Edmond)
  - Cyber System Modeling & Analysis (David, Bill, Saman)
  - Reliability (Bill, Robin)
- Technology Transition Enablers
  - PowerWorld
  - Network Perception
  - TCIPG Industry Relations

# Accomplishments

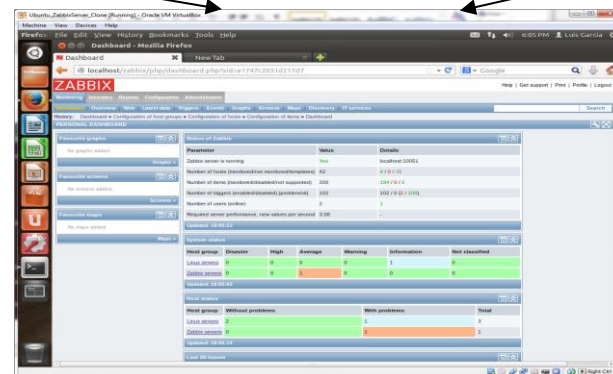
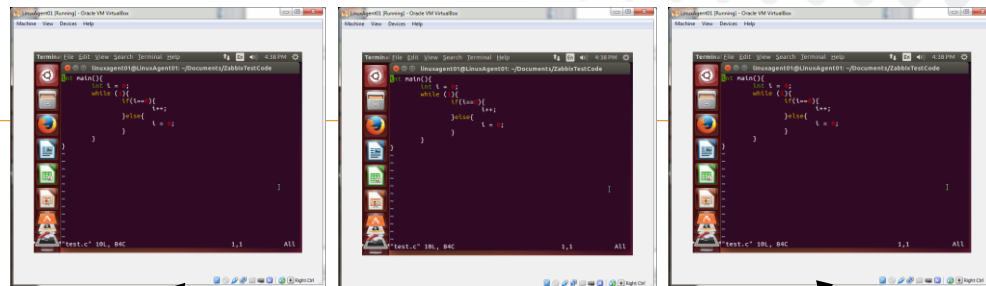
2<sup>nd</sup> Year  
Accomplishments

- ▶ Development of a small synthetic cyber-physical model to facilitate analysis algorithm development and testing
  - 8-susbstation system with associated cyber control network
  - helped development of a language to capture cyber-physical models - Cyber-Physical Topology Language (CPTL)
- ▶ Threat model in the form of attack graph (s) reviewed by industry experts
- ▶ Development of scalable algorithms for analysis model generation
- ▶ Initial prototype of CyPSA framework able to analyze the synthetic cyber-physical model

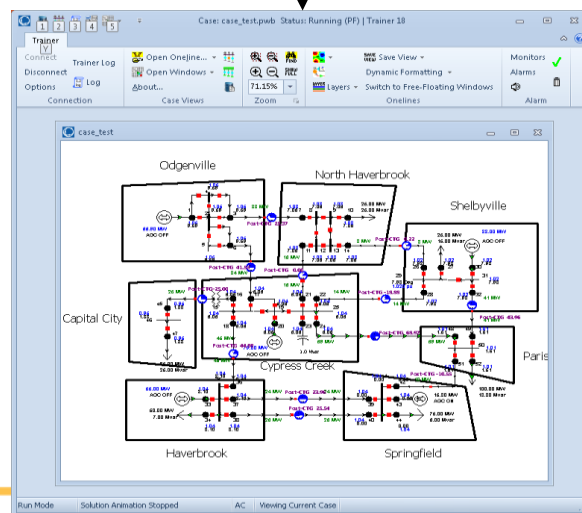
# Development



## Intrusion Detection Sensors

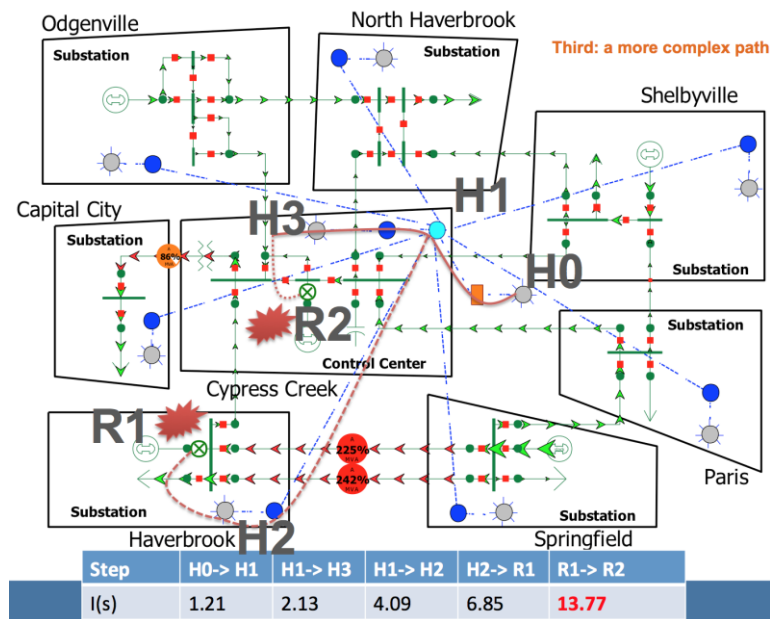


Cyber  
Security  
State  
Estimation



Power Analysis  
(PowerWorld)

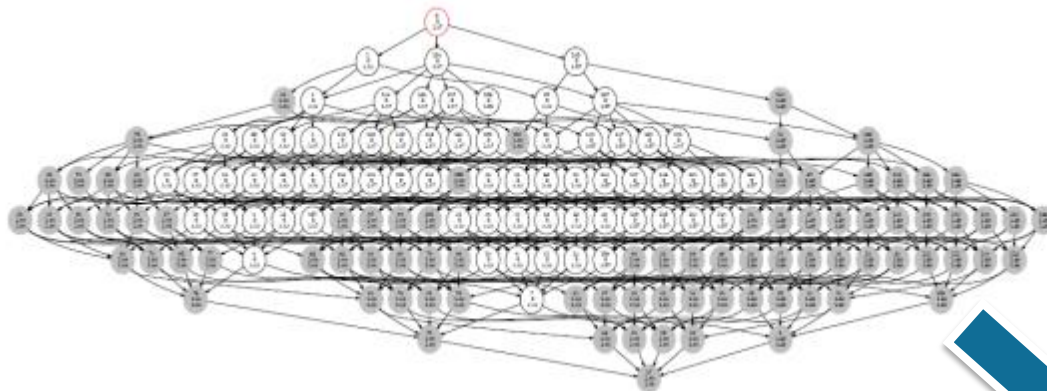
## Automated Model Generation



## Integrated Functional Solution: CyPSA

## Tool Configuration

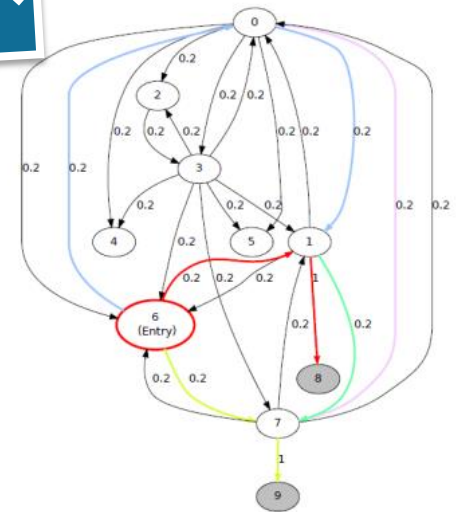
# Scalable Real-Time Analysis



Large detailed model

**Algorithm 1: Cyber-Physical Contingency Selection**  
**Input:** MDP, current\_state, deadline  
**Output:** [ContingencyList]  
1 List  $B \leftarrow \emptyset$ ;  
2 Queue  $Q \leftarrow \emptyset$ ;  
3 for  $s \in S$  do  
4   Color[s]  $\leftarrow$  White;  
5    $F(s) \leftarrow \sum_{i \in L} \{\max\{\frac{f(i)}{\max(i)} - 1, 0\}\}^2$ ;  
6    $I(s) \leftarrow \max_{a \in A(s)} \{\gamma \cdot \sum_{s' \in S} P(s'|s, a) [\Delta F(s, s') + I(s')]\}$ ;  
7 end  
8 Color[current\_state]  $\leftarrow$  Gray;  
9 Enqueue( $Q$ , current\_state);  
10 while (get\_time()  $\leq$  deadline) and ( $Q \neq \emptyset$ ) do  
11    $s \leftarrow$  Dequeue( $Q$ );  
12   for  $a \in A(s)$  do  
13      $R(s, a) \leftarrow \sum_{s' \in S} P(s'|s, a) [\Delta F(s, s') + I(s')]$ ;  
14     Insert( $B$ , [ $R(s, a)$ ,  $s, a$ ]);  
15   end  
16   Sort( $B$ );  
17   Concatenate(ContingencyList,  $B$ );  
18   for  $b \in B$  do  
19     if Color[ $s'_{b,s,b,a}$ ] = White then  
20       Color[ $s'_{b,s,b,a}$ ]  $\leftarrow$  Gray;  
21       Enqueue( $Q$ ,  $s'_{b,s,b,a}$ );  
22     end  
23   end  
24    $B \leftarrow \emptyset$ ;  
25   Color[s]  $\leftarrow$  Black;  
26 end

- Model generation **optimization** resulted in much **smaller models** and **improved performance significantly**



Optimized grid model

Branch-Depth Limit	Analysis Time	Finished Analysis?
5	6 s	yes
10	6 s	yes
15	9 s	yes
20	1 min	yes

Increasing accuracy

- ▶ Getting real cyber-physical models
  - working with a small utility
- ▶ Right level of model abstraction
  - useful analysis results
  - tractable
- ▶ Scaling analysis to deployed system sizes
- ▶ Identifying the right use-cases and associated performance requirements
  - n-1-1
  - proximity to cascading outages
  - what-if scenarios

# Going Forward ...

---

- ▶ Testing with real cyber-physical models
- ▶ Scalability of the analysis
- ▶ Validation and demonstration of technology in lab/field settings
- ▶ Identifying key use-cases and target group in Utilities for tech transition

# Technology-to-Market

---

- ▶ Open to multiple T2M paths (e.g., partners, license, start-up) at this stage
- ▶ Key Partners/Commercialization Channels
  - PowerWorld Corp. and Network Perception
- ▶ Targeting “Operations Technology (OT)” group in utilities
  - Ideally converged OT and IT group

- ▶ Outreach/Presentations
  - Presentation at GridSecCon (October 2014)
  - Presentation at UNITE (March 2014)
  - Presentation to Association of Illinois Electric Co-operatives (October 2014)
  - Presentations at a PSERC meeting and Illinois Power Affiliates meeting (May 2014)
  
- ▶ Engagements-in-the-works
  - Small city utility as an initial test partner
  - Potential participation in GridEx 2015

# Post ARPA-E Goals

---

- ▶ Seek funding to
  - develop validated prototype into a commercial product
  - support development workload to tailor the tool to the needs of initial customers
- ▶ Scalability/Accuracy trade-off is expected to be the risk for large-scale adoption

# Conclusions

---

- ▶ Potential for significant improvement in system resiliency in the face of cyber threats (both accidental and induced)
  - Co-analyze both cyber and power infrastructures
  - Capture inter-dependencies
- ▶ Many challenges need to be overcome
  - Getting data
  - Right modeling abstraction and analysis framework
  - Right use-cases / applications
  - Utility/system operator buy-in